

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 10012790-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): WALKER et al.

Confirmation No.: 9299

Application No.: 09/903,278

Examiner: Tran, Tongoc

Filing Date: July 11, 2001

Group Art Unit: 2134

Title: SYSTEM AND METHOD OF VERIFYING SYSTEM ATTRIBUTES

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on April 6, 2006.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) \$500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month
\$120

☐ 2nd Month
\$450

☐ 3rd Month
\$1020

☐ 4th Month
\$1590

☐ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of \$ 500. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

☒ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:
Commissioner for Patents, Alexandria, VA 22313-1450
Date of Deposit: June 6, 2006

OR

☐ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300.

Date of facsimile:

Typed Name: Cindy C. Dioso

Signature: Cindy C. Dioso

Respectfully submitted,

WALKER et al.

By: James L. Baudino

James L. Baudino

Attorney/Agent for Applicant(s)

Reg No. : 43,486

Date : June 6, 2006

Telephone : 214-855-7544



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

**APPEAL FROM THE EXAMINER TO THE BOARD
OF PATENT APPEALS AND INTERFERENCES**

Applicants: Philip M. WALKER et al. Confirmation No.: 9299
Application Serial No.: 09/903,278
Filed: July 11, 2001
Title: SYSTEM AND METHOD OF VERIFYING SYSTEM
ATTRIBUTES

Group Art Unit: 2134
Examiner: Tran, Tongoc

Docket No.: 10012790-1

MAIL STOP: APPEAL BRIEF PATENTS

Commissioner for Patents

P.O. Box 1450

Alexandria, Virginia 22313-1450

Dear Sir:

APPEAL BRIEF

Applicants have appealed to the Board of Patent Appeals and Interferences from the decision of the Examiner mailed February 7, 2006, finally rejecting Claims 1-26. Applicants filed a Notice of Appeal on April 6, 2006. Applicants respectfully submit herewith this Appeal Brief with authorization to charge the statutory fee of \$500.00.

06/13/2006 HMARZ11 00000006 082025 09903278

01 FC:1401 500.00 DA



REAL PARTY IN INTEREST

The present application was assigned to Hewlett-Packard Company as indicated by an assignment from the inventor recorded on January 9, 2002 in the Assignment Records of the United States Patent and Trademark Office at Reel 012462, Frame 0298. The present application was subsequently assigned to Hewlett-Packard Development Company, L.P. as indicated by an assignment from Hewlett-Packard Company recorded on September 30, 2002 in the Assignment Records of the United States Patent and Trademark Office at Reel 014061, Frame 0492. The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

RELATED APPEALS AND INTERFERENCES

There are no known appeals or interferences that will directly affect or be directly affected by or have a bearing on the Board's decision in this pending appeal.

STATUS OF CLAIMS

Claims 1-26 stand rejected pursuant to a Final Office Action mailed February 7, 2006. Claims 1-26 are presented for appeal.

STATUS OF AMENDMENTS

No amendment has been filed subsequent to the mailing of the Final Office Action.

SUMMARY OF CLAIMED SUBJECT MATTER

Embodiments of the present invention as defined by independent Claim 1 are directed toward a system comprising a target (16), a probe (18, 20) operable to execute in

the target (16) and collect a predetermined set of data associated with the target (16), and a monitor (14) operable to receive the collected predetermined set of data to compare with expected data values to determine whether the target (16) has been altered (at least at page 3, line 15 to page 4, line 17 and page 5, line 10 to page 6, line 21).

Embodiments of the present invention as defined by independent Claim 10 are directed toward a method comprising executing a probe (18, 20) in a target (16) and collecting a predetermined set of data associated with the target (16) for comparison with expected data values for the predetermined set of data to determine whether the target (16) has been altered (at least at page 3, line 15 to page 4, line 17 and page 5, line 10 to page 6, line 21).

Embodiments of the present invention as defined by independent Claim 19 are directed toward a method comprising initiating the execution of a probe (18, 20) in a target (16), receiving from the probe (18, 20) a predetermined set of data associated with the target (16), and comparing the received predetermined set of data with expected data values thereof to determine whether the target (16) has been altered (at least at page 3, line 15 to page 4, line 17 and page 5, line 10 to page 6, line 21).

GROUND OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1-5, 10-14, 19-23, 25 and 26 were rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,499,340 issued to Barritz (hereinafter "*Barritz*") in view of U.S. Patent No. 6,618,735 issued to Krishnaswami et al. (hereinafter "*Krishnaswami*").

2. Claims 6-9, 15-18 and 24 were rejected under 35 U.S.C. 103(a) as being unpatentable over *Barritz* in view of *Krishnaswami* and further in view of Applied Cryptography, Second Edition by Bruce Schneier (hereinafter "*Schneier*").



ARGUMENT

A. Standard

1. 35 U.S.C. § 103

To establish a *prima facie* case of obviousness under 35 U.S.C. § 103, three basic criteria must be met: First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings; second, there must be a reasonable expectation of success; and finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *In re Vaeck*, 947 F.2d 488, (Fed. Cir. 1991); M.P.E.P. § 2143. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *Id.* Further, the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680 (Fed. Cir. 1990); M.P.E.P. § 2143.01. Additionally, not only must there be a suggestion to combine the functional or operational aspects of the combined references, but also the prior art is required to suggest both the combination of elements and the structure resulting from the combination. *Stiftung v. Renishaw PLC*, 945 F.2d 1173, 1183 (Fed. Cir. 1991). Moreover, where there is no apparent disadvantage present in a particular prior art reference, then generally there can be no motivation to combine the teaching of another reference with the particular prior art reference. *Winner Int'l Royalty Corp. v. Wang*, 202 F.3d 1340, 1349 (Fed. Cir. 2000).

B. Argument

1. First Ground of Rejection (Claims 1-5, 10-14, 19-23, 25, and 26)

Claims 1-5, 10-14, 19-23, 25, and 26 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Barritz* in view of *Krishnaswami*. Of the rejected claims, claims 1, 10, and 19 are independent. Applicants respectfully submit that each of independent Claims 1, 10, and 19 are patentable over the cited references and, therefore, Claims 2-5, 11-14, 20-23, 25, and 26 that depend therefrom are also patentable.

Embodiments of the present invention are directed toward a monitor which is used to verify the system attributes of at least one client system to determine whether the client system has been altered in an unauthorized manner. For example, in one embodiment of the present invention, a monitor dispatches a probe to a client system or invokes a copy of the probe disposed in the client system to obtain attribute data associated with the client systems such as a list of system attributes and parameters of client system. The monitor compares the obtained data returned by the probe to determine whether the data matches expected values. If there is a mismatch between the obtained data and a predetermined set of data, there is a possibility that client system has been altered in an unauthorized manner. Accordingly, Claim 1, for example, recites a system comprising “a target,” “a probe operable to execute in the target and collect a predetermined set of data associated with the target,” and “a monitor operable to receive the collected predetermined set of data to compare with expected data values to determine whether the target has been altered.”

In the Final Office Action, the Examiner states that with respect to Claim 1, *Barritz* discloses a system comprising a target, a probe operable to execute in the target and collect a predetermined set of data associated with the target, and a monitor operable to receive the collected predetermined set of data (Final Office Action, page 4 (referring to col. 8, line 65-col. 9, line 8, col. 10, lines 1-22 and line 65 and col. 11, line 24 of *Barritz*)). The Examiner also states that *Barritz* does not explicitly disclose comparing said data with expected data values to determine whether the target has been altered (Final Office Action, page 4), but that *Krishnaswami* discloses comparing information with protected information stored in the database to verify whether information has been altered (Final Office Action, page 4 (referring to *Krishnaswami*, col. 7, lines 9-25)) and that it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the purported teaching of initiating a probe to collect data at a target system to uncover unauthorized usage of product taught by *Barritz* with the teaching integrity file checking purportedly taught by *Krishnaswami* in order to ensure information has not been altered (Final Office Action, page 4). Applicants respectfully disagree.

Independent Claim 1 recites “a probe operable to collect a predetermined set of data associated with the target” and “a monitor operable to receive the collected predetermined set of data to compare with expected data values to determine whether the target has been altered” (emphasis added). As the examiner admits, *Barritz* does not disclose comparing data with expected data values to determine whether a target has been altered. However, the Examiner states that *Krishnaswami* discloses comparing information with protected information stored in the database to verify whether information has been altered (Final Office Action, page 4). Applicants respectfully disagree. *Krishnaswami* appears to disclose a system for protecting existing system files from unauthorized changes using a file-change monitoring component and a system file protection (SFP) service component (*Krishnaswami*, column 5, lines 10-14). *Krishnaswami* appears to disclose that the monitoring component comprises a virtual device driver (Vxd) that is responsible for detecting changes to a protected file and notifying the SFP service component of the change so that the SFP service component can undo the change to the file if the change is determined to be invalid (*Krishnaswami*, column 5, lines 14-19). *Krishnaswami* also appears to disclose that the Vxd (which is used in *Krishnaswami* to detect a change to a protected file) is inserted between the file system manager 86 and the file system drivers 88 of the operating system 70 of the *Krishnaswami* system (*Krishnaswami*, column 5, lines 20-22). *Krishnaswami* recites:

With the Vxd 82 in this position, all calls from the system file manager 86 to the system file drivers 88 for operations on the files stored in the system memory 90 will go through the Vdx. In this way, the Vxd 82 can track all changes to the system files.

(*Krishnaswami* column 5, lines 21-26) (emphasis added). Thus, *Krishnaswami* does not disclose or even suggest “compar[ing] [the received collected predetermined set of data from the probe] with expected data values to determine whether the target has been altered” as recited by Claim 1. To the contrary, the Vxd 82 of *Krishnaswami* (which is used in *Krishnaswami* to detect a change to a protected file) does not compare, nor does it need to compare, any data to detect a change to a file because of its position between the

file system manager 86 and the file system drivers 88 of the operating system 70 of the *Krishnaswami* system. In fact, *Krishnaswami* teaches away from comparing any data to determine whether a file has been altered at least because any calls corresponding to the protected file of *Krishnaswami* automatically go through the Vxd such the Vxd of *Krishnaswami* can detect the change and automatically make a copy of the original file before making the change (*Krishnaswami*, column 5, lines 29-38). Accordingly, for at least this reason, neither *Barritz* nor *Krishnaswami*, alone or in combination, discloses, teaches or suggests the limitations of independent Claim 1.

In the Final Office Action, the Examiner also refers to column 7, lines 9-25, of *Krishnaswami* (Final Office Action, page 4). The portion of *Krishnaswami* referred to by the Examiner appears to be directed toward the SFP service component 80 of *Krishnaswami* (*Krishnaswami*, column 7, lines 9-24). For example, *Krishnaswami* appears to disclose that, in response to the Vxd 82 of *Krishnaswami* detecting a change in a file, the Vxd 82 informs the SFP service component 80 of *Krishnaswami* that a protected file has been changed (*Krishnaswami*, column 5, lines 37-40). *Krishnaswami* also appears to disclose that when the SFP service component 80 receives a message from the Vxd 82 that a protected file has been modified, the SFP service component 80 queries a database 110 for all entries therein that have the same file name as the one modified and determines whether the “new file” is valid (e.g., the new file is deemed valid if (1) it has the same version number as the highest version number of the entries for that file in the database, and (2) it has the correct hash value for that version (*Krishnaswami*, column 7, lines 9-24). Thus, the SFP service component 80 of *Krishnaswami* also does not compare any data to “determine whether the target has been altered” as recited by Claim 1. To the contrary, the SFP service component 80 appears to be used only after a change to a file in the *Krishnaswami* has already been detected. Thus, for at least this reason also, Claim 1 is patentable over the cited references.

Moreover, Applicants respectfully submit that there is no motivation or suggestion to combine purported reference teachings as proposed by the Examiner. For example, *Barritz* is directed toward a method and apparatus for monitoring computer

program usage (*Barritz*, abstract). *Barritz* appears to disclose a software product to detect, monitor and report on software products installed on a computer system and their actual usage (*Barritz*, column 2, lines 57-60) (emphasis added). *Barritz* appears to disclose that the software product of *Barritz* “automatically determin[es] and record[s] each instance of actual usage of particular software products, as well as the identity of each user of those products” (*Barritz*, column 2, lines 62-65) (emphasis added). *Barritz* appears to disclose a surveying program to examine all the storage devices of a computer system to determine the program modules present (*Barritz*, column 4, lines 28-33). *Barritz* further appears to disclose a monitoring program that records pertinent information in a recorded information log when certain events occur (“for each module used, the information recorded by the monitor consists of the module name, the library name from which it was loaded, the volume of the library, the product ID, the job name using the module” (*Barritz*, column 6, lines 32-53)). *Barritz* also appears to disclose a reporting program for reporting the events logged by the monitoring program (“sorts, correlates, consolidates, summarizes, formats and outputs reports” (*Barritz*, column 8, lines 11-17)). Thus, the information desired by the *Barritz* system is actual usage of a program module of *Barritz* (“mak[ing] it possible to for a company to cancel maintenance or rental on unused or under-used products” (*Barritz*, column 2, lines 65-67)).

In the Final Office Action, the Examiner asserts that the basis for combining purported reference teachings is “to uncover unauthorized usage of the [*Barritz*] product” (Final Office Action, page 4). Applicants respectfully point out that “unauthorized usage” as stated by the Examiner as a basis for combining purported reference teachings does not require there to be an “altered” target as recited by Claim 1. To the contrary, unauthorized usage of the *Barritz* system may result independently of whether or not the *Barritz* system is altered. Therefore, Applicants respectfully submit that there is no motivation or suggestion to combine purported reference teachings as proposed by the Examiner. Further, even if the information in the *Barritz* system corresponding to actual usage of a program module of *Barritz* is compared with predetermined data, which Applicants respectfully submit is neither taught nor

suggested, the resulting comparison would still not be determinative of whether the *Barritz* system was altered as unauthorized usage of the *Barritz* system may result independently of whether or not the *Barritz* system is altered. Clearly, the Examiner is using hindsight reconstruction to piece together purported teachings of the cited references to arrive at Applicants' claimed invention, which is improper. Moreover, even if the purported teaching of the cited references are combined, the resulting combination still does not disclose, teach or suggest the limitations of Claim 1. Accordingly, for at least these reasons also, Applicants respectfully submit that Claim 1 is patentable over the cited references.

Independent Claim 10 recites “executing a probe in a target” and “collecting a predetermined set of data associated with the target for comparison with expected data values for the predetermined set of data to determine whether the target has been altered” (emphasis added), and independent Claim 19 recites “initiating the execution of a probe in a target,” “receiving from the probe a predetermined set of data associated with the target” and “comparing the received predetermined set of data with expected data values thereof to determine whether the target has been altered” (emphasis added). At least for the reasons discussed above in connection with independent Claim 1, Applicants respectfully submit that independent Claims 10 and 19 are also patentable over the cited references.

Accordingly, at least for the reasons discussed above, independent Claims 1, 10, and 19 are clearly patentable of the cited references. Therefore, Claims 1, 10, and 19, and Claims 2-9, 11-18, and 20-26 that depend respectively therefrom, are in condition for allowance.

2. Second Ground of Rejection (Claims 6-9, 15-18, and 24)

Claims 6-9, 15-18 and 24 were rejected under 25 U.S.C. § 103 as being unpatentable over *Barritz* in view of *Krishnaswami* and further in view of *Schneier*.

Claims 6-9, 15-18 and 24 depend respectively from independent Claims 1, 10 and 19. As discussed above, Claims 1, 10 and 19 are patentable over the *Barritz* and *Krishnaswami* references. Moreover, *Schneier* does not appear to remedy, nor did the Examiner rely on *Schneier* to remedy, at least the deficiencies of the *Barritz* and *Krishnaswami* references discussed above. Therefore, for at least this reason, Claims 6-9, 15-18 and 24 are patentable over the cited references.

Additionally, in the Final Office Action, the Examiner states that with respect to Claims 6-9, for example, *Schneier* purportedly discloses using a digital signature with encryption to authenticate the integrity of data transmitted over the network, and that it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of *Barritz*'s monitoring computer usage over the network with *Schneier*'s purported teaching of digital signature to authenticate the data received to ensure the integrity of the data transmitted over the network (Final Office Action, page 4 (citing *Schneier*, pages 30-31, 41-44 and 48-50)). Applicants respectfully disagree.

Claim 6, for example, recites "wherein the probe is operable to calculate a signature value of at least a portion of an execution image of the probe" (emphasis added). Applicants also direct the Examiner to at least page 3, lines 9-11, of Applicants' specification which recites: "In order to verify that the resident probe program itself has not been tampered with, a hash or digital signature of the probe program is generated to ensure it is the original program." (emphasis added). The Examiner appears to rely on *Schneier* to "authenticate the integrity of data transmitted over the network" (Final Office Action, page 6). However, Claim 6 for example, especially when read in view of Applicants' specification, is directed toward ensuring the integrity of the probe program at a target. Therefore, Applicants respectfully submit that *Barritz*, *Krishnaswami* and

Schneier, alone or in combination, do not disclose, teach or suggest the limitations of Claim 6. Further, for at least the reasons discussed above in connection with Claim 6, Applicants respectfully submit that *Barritz*, *Krishnaswami* and *Schneier*, alone or in combination, do not disclose, teach or suggest the limitations of Claims 7-9, 15-18 and 24.

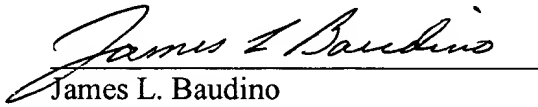
Accordingly, Applicants respectfully submit that Claims 6-9, 15-18 and 24 are patentable over the cited references.

CONCLUSION

Applicants have demonstrated that the present invention as claimed is clearly distinguishable over the art cited of record. Therefore, Applicants respectfully request the Board of Patent Appeals and Interferences to reverse the final rejection of the Examiner and instruct the Examiner to issue a notice of allowance of all claims.

The Commissioner is authorized to charge the statutory fee of \$500.00 to Deposit Account No. 08-2025 of Hewlett-Packard Company. Although no other fee is believed due, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 08-2025 of Hewlett-Packard Company.

Respectfully submitted,


James L. Baudino
Registration No. 43,486

Date: June 6, 2006

Correspondence To:

L. Joy Griebenow
Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400
Tel. (970) 898-3884



CLAIMS APPENDIX

1. A system comprising:
a target;
a probe operable to execute in the target and collect a predetermined set of data associated with the target; and
a monitor operable to receive the collected predetermined set of data to compare with expected data values to determine whether the target has been altered.
2. The system, as set forth in claim 1, wherein the probe is resident in the target.
3. The system, as set forth in claim 1, wherein the monitor is operable to send the probe to the target for execution.
4. The system, as set forth in claim 1, wherein the probe repeatedly executes and the predetermined set of data varies for each execution of the probe.
5. The system, as set forth in claim 1, wherein the predetermined set of data includes system attributes and system usage data.
6. The system, as set forth in claim 1, wherein the probe is operable to calculate a signature value of at least a portion of an execution image of the probe.
7. The system, as set forth in claim 1, wherein the monitor is operable to compare the calculated signature value to an expected signature value.
8. The system, as set forth in claim 1, wherein the probe is operable to determine a signature value of a random subset of an execution image of the probe.

9. The system, as set forth in claim 1, wherein the probe is operable to generate an encryption key from the signature value for encrypting the collected predetermined set of data.

10. A method comprising:

executing a probe in a target;

collecting a predetermined set of data associated with the target for comparison with expected data values for the predetermined set of data to determine whether the target has been altered.

11. The method, as set forth in claim 10, further comprising receiving a request to execute the probe resident in the target.

12. The method, as set forth in claim 10, further comprising receiving the probe and executing the received probe in the target.

13. The method, as set forth in claim 10, wherein the step of executing a probe is repeated.

14. The method, as set forth in claim 10, wherein the step of executing a probe comprises collecting a different predetermined set of data for each execution of the probe.

15. The method, as set forth in claim 10, further comprising calculating a signature value of at least a portion of the probe for comparison to an expected signature value.

16. The method, as set forth in claim 10, further comprising calculating a signature value of the probe for comparison to an expected signature value.

17. The method, as set forth in claim 16, further comprising:
generating an encryption key from the signature value; and
encrypting the collected predetermined set of data with the encryption key.

18. The method, as set forth in claim 17, further comprising:
sending the encrypted data to a monitor, the data including system attribute data
and system usage data;
decrypting the encrypted data using a decryption key;
verifying the system attribute data; and
generating billing data based on the system usage data in response to the system
attribute data being verified.

19. A method comprising:
initiating the execution of a probe in a target;
receiving from the probe a predetermined set of data associated with the target;
and
comparing the received predetermined set of data with expected data values
thereof to determine whether the target has been altered.

20. The method, as set forth in claim 19, further comprising sending a request to
the probe resident in the target to initiate the execution.

21. The method, as set forth in claim 19, further comprising sending the probe
and executing the probe in the target.

22. The method, as set forth in claim 19, wherein initiating the execution of a
probe comprises repeating execution of the probe.

23. The method, as set forth in claim 19, wherein initiating the execution of a
probe comprises collecting a different predetermined set of data for each execution of the
probe.

24. The method, as set forth in claim 19, further comprising:

receiving collected data encrypted by the probe using an encryption key derived from a self-hash value, the data including system attribute data and system usage data; decrypting the encrypted data; and verifying the system attribute data.

25. The method, as set forth in claim 23, further comprising generating billing data based on the system usage data in response to the system attribute data being verified.

26. The method, as set forth in claim 19, further comprising:

receiving a reply containing at least the collected predetermined set of data, the data including system attribute data and system usage data; and verifying the system attribute data.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None